REMARKS/ARGUMENTS

Claims 1-31 are pending, claims 1-27 were canceled. Consequently, claims 28-31 remain pending. Claims 1-27 were canceled to more particularly claim the subject matter of the present invention from the point of view of the indicia generating devices, and were not canceled in light of the references cited by the Examiner. Accordingly, no subject matter of the present invention is meant to be disclaimed or dedicated public due to cancellation of the claims.

The Examiner rejected claims 1-31 under 35 USC §103(a) as being unpatentable over US patent 5,812,666 to Baker et al. in view of US patent 6,295,359 to Cordery et al. Applicant respectfully disagrees.

The present invention provides a method and system for dispensing and evidencing indicia by an indicia generating device in a system having a plurality of indicia generating devices that have been divided into n groups. In a preferred embodiment, the system includes a key distribution center 24, a plurality of postage generating devices 14, and multiple USPS distribution centers 20. The key distribution center divides the postage generating devices (PDGs) into n groups corresponding to different geographic designations (e.g., zip codes), and assigns a set of verification keys, V_i, to each PGD group, where each verification key in the set is encrypted as a function of one of the corresponding destination region. The key distribution center also assigns a set of key ID's 23 to each PDG group, where each key ID in the set is associated with one of the assigned verification keys and is encrypted as a function of the same destination region used to encrypt the corresponding verification key. After assigning the verification keys 21 to the PGD groups 26, the KDC 24 distributes to each distribution center the sets of verification keys 21 and key ID's 23 that were encrypted as a function of the corresponding destination region.

The PDGs generate the indicia that is marked on media, such as postage, and the distribution centers verify the indicia when the media is received through the mail. Rather than transmitting the verification keys and key ID's to the PDG, each PDG generates one of the verification keys and corresponding key ID from the set of keys assigned to its group based on a particular destination. This is accomplished as described with respect to Figure 5.

The process begins in step 70 when the PDG's receive a master secret key K and a secret key K_i from the KDC 24. In response to receiving a request from a user to generate an indicium for a mail piece destined for a particular destination *Dest*, the indicium is generated in step 72, and the verification key V_i^{Dest} is computed in step 74 as a function of the secret key K_i and the destination. The PGD 14 also computes the encrypted key ID I_i^{Dest} as a function of the destination in step 76. The PGD 14 evidences the indicia in step 78 by creating a digital signature for the indicia using the verification key V_i^{Dest} and digitally signs the indicia by including the digital signature and the computed index I_i^{Dest} on the indicia. The mail piece bearing the postage indicia is now ready for mailing and subsequent verification. These are the steps recited in claim 28.

In addition, according to the preferred embodiment of the invention, postage validation is performed at destination distribution centers, rather than at originating distribution centers, using the verification keys, which are encrypted as a function of the destination and are only distributed to the corresponding distribution centers.

The Examiner relies on a combination of Baker and Cordery for teaching the claimed invention. It is respectfully submitted that a combination of Baker and Cordery fail to teach or suggest the combination of elements recited in independent claim 28.

Baker provides a key management system that distributes cryptographic keys to digital meters for multiple domains, including vendor keys and postal keys for a plurality of countries. The key management system is configured to prevent translation of keys between domains, to provide assurance in a domain that the keys were generated in the domain, and that each key has been installed in only one meter by the system (col. 3, lines 23-31). The key management system includes separate logical security domains: one vendor domain and or one more postal domains. Each domain provides a full set of key generation, key distribution, key installation and token verification services (col. 5, lines 24-27). Vendor data keys are generated at a vendor data center (col. 5, lines 42-54), and postal keys are generated at a postal data center (col. 6, lines 5-14).

Both vendor and postal master keys are installed in the digital meters (col. 6, lines 43-47), and each digital meter receives the vendor master key and postal master key while physically located in the vendor manufacturing facility before distribution (col. 6, lines 52-56). To enforce a security requirement that a master key can only be attempted or installed in any digital meter once, each master key is identified by a domain master key identification number (col. 7, lines 18-58). Domain keys are used to encrypt the domain master keys (vendor and postal) (col. 6, lines 61-63). The main keys are encrypted by domain Key set 103, which consist of a RSA key pair for confidentiality and an RSA key pair for authentication (col. 8, lines 4-15.)

Earth domain digital meters are made country specific after manufacturing (col. 9, lines 55-57). Earth domain master keys are generated and installed into Earth domain digital meters. Earth domain digital meters are assigned to a country specific security domain (col. 10, lines 11-15). The domain master key is encrypted with the country specific secret key (col. 10, lines 29-31).

In operation, each meter uses the domain master key to generate a temporal key, referred to as a token key for each domain, which is used to generate a token from mail piece data. Postal temporal keys distributed to postal verification sites are used for local verification of the indicia (col. 18, lines 23-34).

Cordery provides a method and apparatus for distributing keys in a public-key system utilized in a postage metering environment that generates a set of one or more master keys, and calculates for each master private key, a corresponding master public key. In each of the postage metering devices, a corresponding device private key is installed that is derived is a linear combination of at least two of the master private keys from the set of master private keys (Col. 2, lines 52-67).

In contrast, claim 28 of the present invention recites a method for dispensing and evidencing postage indicia by a postage generating device (PGD) in a system having a plurality of PGDs that have been divided into n groups identified by a group designation G_i, $i = 1,...n$. Each of the steps in claim 28 is performed by the indicia generating devices. It is respectfully submitted that the neither Baker or Cordery, singularly or in combination, teach or suggest the combination of elements recited in claim 28.

During the rejection of claims 1-31, the Examiner stated that Cordery teaches receiving a public master key and a key matrix that meets the recitation of receiving "a master secret key K and a secret key K_i," as recited in step (a). To support the rejection, the Examiner cited Cordery column 6, lines 39-63. However, this passage Cordery merely states:

> A key management facility 3 includes a key generation box 5 which preferably randomly generates a set of private master postage meter keys (step S1) and calculates a corresponding set of public master postage meter keys based on the private master postage meter keys (step S3). Both the generated private and public master postage meter keys are stored (step S5) in a secure data base 7. The public master postage meter keys are sent to individual verifying sites 9 which

verify the postage indicium on mailpieces as is discussed in more detail below (step S7). Referring specifically to FIGS. 3 and 5, a postage meter key calculator 11 utilizes a meter key matrix or a matrix algorithm defined in accordance with the previously described instant invention (step S9) to determine for each manufactured meter 13 (step S11) the row of coefficients for that particular meter 13 (step S13). The row of coefficients are then used to calculate a private key for the particular meter 13 utilizing a linear combination of at least more than one of the public master postage meter keys (step S15). The calculated private postage meter key for a particular postage meter 13 is then stored within the postage meter 13 (step S17). The key matrix or matrix algorithm is also provided to the verifying sites 9 for subsequent use in generating the postage meter public keys as discussed below (step S18).

It is respectfully submitted that this passage fails to teach or suggest the combination of elements recited in claim 28. For example, although Cordery discloses that a private key calculated for a particular postage meter is stored within the postage meter, Cordery fails to disclose that a "secret key" is also stored within the postage meter. Cordery discloses the use of other keys, such as public keys and a key matrix, but the public keys are sent to individual verifying sites, not the meters; and key matrix is used by a postage meter key calculator and a key management facility, not the meters. Cordery also fails to teach or suggest that the meters/PGDs have been divided into n groups identified by a group designation, "G_i, $i = 1,...n$", and the meters in each group receive "a secret K_i," corresponding to the Group designation, as required by step (a). Cordery's private/public keys and/or the key matrix also fail to perform the functions of the master secret key K and a secret key K_i, as recited in steps (c) through (f).

Because Cordery's private/public keys and/or the key matrix fail to teach or suggest the functions of the master secret key K and a secret key K_i, as recited in claim 28, Cordery fails to cure the deficiencies of Baker, and a combination of Baker and Cordery likewise fail to teach or suggest the recitations of claim 28.

For completeness and clarity, Applicant would further like to point out that none of Baker's disclosed keys teach or suggest the keys and functionality of the keys recited in claim 28. For example, Baker fails to teach or suggest that each of the indicia generating devices receives "a master secret key K and a secret key K_i," as recited in step (a). Although Baker teaches that Earth domain digital meters are assigned a country specific security domain and receive copies of Earth domain master keys that are encrypted with a country specific secret key, Baker fails to teach or suggest that meters in each group designation, "G_i, $i = 1,...n$", also receive "a secret K_i," corresponding to that Group designation, as required by step (a).

In addition, it is believed that Baker's country specific secret keys cannot be considered analogous to the recited secret K_i because Baker's country specific secret keys are not believed to be installed in the meters. In addition, Baker's country specific secret keys are not used by the meters to "comput[e] a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination (*Dest*), as recited in step (c).

With further regard to step (c), it is noted that Baker discloses that each meter uses the domain master key to generate a temporal key, referred to as a token key, for each domain, which is used to generate a token from mail piece data. However, it is not believed either Baker's master key or the temporal key is analogous to the verification key. Baker's master key is not analogous because it is already present in the meter, is not computed as a function of the secret key and the postal destination, as required by step (c), and is not used "to create a digital signature for the indicia", as recited in step (e). Instead, Baker's temporal key is used to generate the token from mail piece data. It is believed Baker's temporal key is not analogous to the claimed verification key because although the temporal key is computed from one key (the

domain master key), it is not computed as a function of a second key, the "secret key", and the postal destination, as required by step (c).

Based on the foregoing, it is respectfully submitted that a combination of Baker and Cordery fail to teach or suggest independent claims 28-31. In view of the foregoing, it is submitted that claim 28 is allowable over the cited references. Because the secondary references stand or fall with the primary references, claims 28-31 are allowable because they are dependent upon the allowable independent claim. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 28-31 as now presented.

Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

April 6, 2005
Date

Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540